Amendments to the CLAIMS:

Without prejudice, this listing of the claims replaces all prior versions and listings of the claims in the present application:

LISTING OF CLAIMS:

1-71. (Canceled).

72. (New) A data storing method of storing digital information which has a value, the data storing method is used in a system including an issuer apparatus issuing the digital information and a user apparatus, the method comprising:

adding, by the issuer apparatus, a signature to the digital information;

generating, by the issuer apparatus, a manifest corresponding to the digital information;

generating, by the issuer apparatus, accreditation information with the signature, and sending the digital information with the signature and the accreditation information with the signature to the user apparatus, wherein the accreditation information indicates third parties that are trusted by the issuer apparatus and that trust the user apparatus;

receiving, by the issuer apparatus, session information from the user apparatus, and sending information that includes the manifest and the session information, to the user apparatus; and

verifying, by the user apparatus, the manifest and the session information, and storing the manifest in the user apparatus only when the manifest and the session information are verified.

73. (New) A user apparatus for storing digital information having a value that is issued by an issuer apparatus, comprising:

first storing means for storing the digital information with a signature of the issuer apparatus and accreditation information, wherein the digital information with the signature and the accreditation information are received from the issuer apparatus or from a second user

apparatus, and the accreditation information indicates third parties that are trusted by the issuer apparatus and that trust the user apparatus;

second storing means for storing a manifest corresponding to the digital information, wherein the manifest is received from the issuer apparatus or from the second user apparatus;

first authentication means for verifying the manifest; and

first control means for storing the manifest into the second storing means only if the first authentication means determines that the manifest is valid.

74. (New) The user apparatus as claimed in claim 73, wherein the second storing means and the first authentication means are tamper-proof.

75. (New) The user apparatus as claimed in claim 73, wherein, when the user apparatus moves the manifest from the second storing means to another apparatus, the user apparatus extracts the manifest from the second storing means and deletes the manifest from the second storing means.

a1

76. (New) The user apparatus as claimed in claim 73, further comprising:

session information generation means for generating unique session information that includes a verification key of the user apparatus and a serial number, wherein the session information is held in the user apparatus, and is sent to the second user apparatus;

wherein the user apparatus receives the session information in addition to the manifest from the second user apparatus and verifies the received session information by using the held session information.

77. (New) An issuer apparatus for issuing digital information which has a value, the issuer apparatus comprising:

accreditation information generation means for generating accreditation information which includes a set of information representing third parties that are trusted by the issuer of the digital information;

signature means for providing a signature to the digital information and to the accreditation information;

manifest generation means for generating a manifest corresponding to the digital information;

means for sending the digital information and the accreditation information to a user apparatus;

means for receiving session information which includes a verification key of the user apparatus and a serial number; and

means for sending information including a verification key of the issuer apparatus, the manifest and the session information to the user apparatus.

78. (New) A collector apparatus for exercising a right of digital information which has a value that is issued by an issuer apparatus, the collector apparatus comprising:

means for receiving, from a user apparatus, the digital information with a signature of the issuer apparatus and accreditation information with the signature, wherein the accreditation information indicates third parties that are trusted by the issuer apparatus and that trust the user apparatus;

a1

means for generating unique session information and sending the session information to the user apparatus;

means for receiving information including a manifest corresponding to the digital information and the session information from the user apparatus; and

means for verifying the session information, the manifest and the accreditation information.

79. (New) A data storing system for storing digital information which has a value, the data storing system, comprising:

a user apparatus for using digital information;

an issuer apparatus for issuing digital information; and

a collector apparatus for exercising a right of digital information;

the user apparatus including:

first storing means for storing the digital information with a signature of the issuer apparatus and accreditation wherein the digital information with the signature and the accreditation information are received from the issuer apparatus or from a

second user apparatus, and the accreditation information indicates third parties that are trusted by the issuer apparatus and that trust the user apparatus;

second storing means for storing a manifest corresponding to the digital information, wherein the manifest is received from the issuer apparatus or from the second user apparatus;

first authentication means for verifying the manifest; and

first control means for storing the manifest into the second storing means only if the first authentication means determines that the manifest is valid;

the issuer apparatus including:

accreditation information generation means for generating the accreditation information;

signature means for providing a signature to the digital information and to the accreditation information;

manifest generation means for generating the manifest corresponding to the digital information;

a1

means for sending the digital information and the accreditation information to the user apparatus;

means for receiving session information which includes a verification key of the user apparatus and a serial number; and

means for sending information including a verification key of the issuer apparatus, the manifest and the session information to the user apparatus;

the collector apparatus including:

means for receiving, from the user apparatus, the digital information with the signature of the issuer apparatus and the accreditation information with the signature,

means for generating unique session information and sending the session information to the user apparatus;

means for receiving information including the manifest corresponding to the digital information and the session information from the user apparatus; and

means for verifying the session information, the manifest and the accreditation information.

80. (New) A computer readable medium storing program code for causing a computer to store digital information which has a value that is issued by an issuer apparatus, the computer being used as a user apparatus, the computer readable medium comprising:

first storing program code means for storing the digital information with a signature of the issuer apparatus and accreditation information in a first storage, wherein the digital information with the signature and the accreditation information are received from the issuer apparatus or from a second user apparatus, and the accreditation information indicates third parties that are trusted by the issuer apparatus and that trust the user apparatus;

second storing program code means for storing a manifest corresponding to the digital information in a second storage, wherein the manifest is received from the issuer apparatus or from the second user apparatus;

first authentication program code means for verifying the manifest; and

first control program code means for storing the manifest into the second storage only if the first authentication program cede means determines that the manifest is valid.

81. (New) The computer readable medium as claimed in claim 80, wherein the second storage is tamper-proof.

82. (New) The computer readable medium as claimed in claim 80, further comprising program code means for extracting the manifest from the second storage and deletes the manifest from the second storage when the manifest is transferred from the second storage to another apparatus.

83. (New) The computer readable medium as claimed in claim 80, further comprising:

session information generation program code means for generating unique session information, that includes a verification key of the user apparatus and a serial number, wherein the session information is held in the user apparatus, and is sent to the second user apparatus;

wherein the user apparatus receives the session information in addition to the manifest from the second user apparatus and verifies the received session information by using the information.

84. (New) A computer readable medium storing program code for causing a computer to issue digital information which has a value, the computer being used as an issuer apparatus, the computer readable medium comprising:

accreditation information generation program code means for generating accreditation information which includes a set of information representing third parties that are trusted by the issuer of the digital information;

signature program code means for providing a signature to the digital information and to the accreditation information;

manifest generation program code means for generating a manifest corresponding to the digital information;

program code means for sending the digital information and the accreditation information to a user apparatus;

program code means for receiving session information which includes a verification key of the user apparatus and a serial number; and

program code means for sending information including a verification key of the issuer apparatus, the manifest and the session information to the user apparatus.

85. (New) A computer readable medium storing program code for causing a computer to exercise a right of digital information which has a value issued by an issuer apparatus, the computer being used as a collector apparatus, the computer readable medium comprising:

program code means for receiving, from a user apparatus, the digital information with a signature of the issuer apparatus and accreditation information with the signature, wherein the accreditation information indicates third parties that are trusted by the issuer apparatus and that trust the user apparatus;

program code means for generating unique session information and sending the session information to the user apparatus;

program code means for receiving information including a manifest corresponding to the digital information and the session information from the user apparatus; and

program code means for verifying the session information, the manifest and the accreditation information.

86. (New) An original data circulation method in an original data circulation system for storing or circulating original data which is digital information, the method comprising:

sending, by a first apparatus, originality information to a second apparatus, the originality information including a fingerprint corresponding to a source apparatus of the original data and second information corresponding to the original data, and

performing an authentication step of identifying and authenticating, by the second apparatus, the source apparatus, verifying whether the source apparatus is the same as an apparatus corresponding to the fingerprint, and determining that the originality information is valid if the source apparatus is the same as an apparatus corresponding to the fingerprint.

87. (New) The original data circulation method as claimed in claim 86, wherein:

the source apparatus conceals a secret key, and the fingerprint is a hash value generated by applying a unidirectional function to a public key of the source apparatus; and

the second apparatus authenticates the source apparatus by verifying that the source apparatus has a private key corresponding to the fingerprint.

88. (New) The original data circulation method as claimed in claim 86, wherein:

the sending includes sending a third party certificate to the second apparatus, the third party certificate being a certificate representing that the second apparatus is authenticated by a third party; and

the second apparatus authenticates the first apparatus by verifying that the third party certificate authenticates the first apparatus and that a certifier in the third party certificate is included in third parties stored in the second apparatus.

89. (New) The original data circulation method as claimed in claim 86, wherein:

the first apparatus conceals a private key of the first apparatus, and in the sending, the first apparatus sends, to the second apparatus, a public key certificate and a first signature corresponding to the private key, wherein the public key certificate is generated by adding, to a public key corresponding to the private key, a second signature of a third party which trusts the first apparatus; and

in the authentication, the second apparatus verifies the first signature by using the public key included in the public key certificate, and verifies whether a hash value of a public key of the third party is included in fingerprints of third parties stored in the second apparatus.

90. (New) The original data circulation method as claimed in claim 86, wherein:

the second apparatus includes accreditation information that indicate one or a plurality of source apparatuses trusted by the second apparatus, and

in the authentication, the second apparatus verifies whether the fingerprint of the source apparatus of the original data is included in the accreditation information.

91. (New) An original data circulation system for storing or circulating original data which is digital information, the system comprising:

a first apparatus which includes sending means for sending originality information, the originality information including a fingerprint corresponding to a source apparatus of the original data and second information corresponding to the original data; and

a second apparatus which includes authentication means for identifying and authenticating the source apparatus of the original data, and means for verifying whether the source apparatus is the same as an apparatus corresponding to the fingerprint, and determining that the originality information is valid if the source apparatus is the same as an apparatus corresponding to the fingerprint.

92. (New) The original data circulation system as claimed in claim 91, wherein:

the source apparatus conceals a secret key, and the fingerprint is a hash value generated by applying a unidirectional function to a public key of the source apparatus; and

the second apparatus authenticates the source apparatus by verifying that the source apparatus has a private key corresponding to the fingerprint.

93. (New) The original data circulation system as claimed in claim 91, wherein:

the sending means includes means for sending a third party certificate to the second apparatus, the third party certificate being a certificate representing that the second apparatus is authenticated by a third party; and

the second apparatus authenticates the first apparatus by verifying that the third party certificate authenticates the first apparatus and that a certifier in the third party certificate is included in third parties stored in the second apparatus.

94. (New) The original data circulation system as claimed in claim 91, wherein:

the first apparatus conceals a private key of the first apparatus, and the first apparatus sends, to the second apparatus, a public key certificate and a first signature corresponding to the private key, wherein the public key certificate is generated by adding, to a public key corresponding to the private key, a second signature of a third party which trusts the first apparatus; and

the second apparatus verifies the first signature by using the public key included in the public key certificate, and verifies whether a hash value of a public key of the third party is included in fingerprints of third parties stored in the second apparatus.

95. (New) The original data circulation system as claimed in claim 91, wherein:

the second apparatus includes means for storing or obtaining accreditation information that indicate one or a plurality of source apparatuses trusted by the second apparatus; and

the second apparatus verifies whether the fingerprint of the source apparatus of the original data is included in the accreditation information.

96. (New) An issuer apparatus in an original data circulation system for storing or circulating original data which is digital information, the issuer apparatus comprising:

originality information generation means for generating originality information which includes a fingerprint corresponding to the issuer apparatus and second information corresponding to the original data; and

originality information sending means for sending the originality information.

97. (New) The issuer apparatus as claimed in claim 96, comprising:

means for concealing a private key; and

means for generating a hash value of a public key corresponding to the key as the fingerprint.

98. (New) The issuer apparatus as claimed in claim 96, comprising means for generating the second information by applying an unidirectional function to the original data.

99. (New) The issuer apparatus as claimed in claim 98, wherein the second information is an identifier which identifies contents in a network.

100. (New) A user apparatus in an original data circulation system for storing or circulating original data which is digital information, the user apparatus comprising:

originality information sending means for sending originality information which includes a fingerprint corresponding to a source apparatus of the original data and second information corresponding to the original data;

identifying means for identifying the source apparatus of the originality information;

authentication means for determining that the originality information is valid if the source apparatus is authenticated and an apparatus corresponding to the fingerprint and the source apparatus are the same; and

storing means for storing the originality information if the authentication means determines that the originality information is valid.

101. (New) The user apparatus as claimed in claim 100, comprising means for deleting the originality information if the user apparatus sends the originality information to another apparatus.

102. (New) A collector apparatus in an original data circulation system for storing or circulating original data which is digital information, the collector apparatus comprising:

identifying means for identifying a source apparatus of originality information;

authentication means for authenticating the source apparatus; and

data processing means for performing a process corresponding to the original data if the authentication means determines that the originality information which is sent to the collector apparatus is valid.

103. (New) The collector apparatus as claimed in claim 102, wherein:

the collector apparatus includes means for storing or obtaining issuer information; and

the data processing means performs a process corresponding to the original data if the authentication means determines that the originality information which is sent to the collector apparatus is valid and if a fingerprint included in the originality information is included in the issuer information.

104. (New) An original data circulation system for storing or circulating original data which is digital information, the original data circulation system comprising:

an issuer apparatus which includes means for generating originality information and sending the originality information, the originality information including a fingerprint corresponding to the issuer apparatus and second information corresponding to the original data;

a user apparatus which includes means for verifying validity of a source apparatus of the originality information and means for storing the originality information when the validity is verified; and

a collector apparatus which includes means for verifying validity of a source apparatus of the originality information and data processing means for performing a process on the original data if the validity is verified.

105. (New) An original data circulation system for storing or circulating original data which is digital information, the original data circulation system comprising:

an issuer apparatus including:

first originality information generation means for generating originality information which includes a fingerprint corresponding to the issuer apparatus and second information corresponding to the original data; and

first originality information sending means for sending the originality information;

a user apparatus including:

first originality information sending means for sending the originality information;

first identifying means for identifying a source apparatus of the originality information;

first authentication means for determining that the originality information is valid if the source apparatus is authenticated and an apparatus corresponding to the fingerprint and the source apparatus are the same; and

storing means for storing the originality information when the first authentication means determines that the originality information is valid; and

a collector apparatus including:

second identifying means for identifying a source apparatus of originality information;

second authentication means for authenticating the source apparatus; and

data processing means for performing a process corresponding to the original data if the second authentication means determines that the originality information which is sent to the collector apparatus is valid.

106. (New) The original data circulation system as claimed in claim 104, wherein:

the apparatus includes means for sending, to the issuer apparatus, the originality information received from the user apparatus; and

the issuer apparatus includes:

means for verifying that the originality information is generated by the issuer apparatus;

means for verifying that the originality information is sent via a valid route;

means for verifying that the original data corresponding to the second information has been processed by the data processing means; and

means for providing a value according to the original data to the collector apparatus.

107. (New) The original data circulation system as claimed in claim 104, wherein:

the issuer apparatus includes means for adding a usable number of the original data as count information to the originality information;

the user apparatus includes means for verifying the count information, wherein the user apparatus can use the data the usable number of times; and

the collector apparatus includes means for verifying the count information.

.

108. (New) The original data circulation system as claimed in claim 104, wherein:

the user apparatus sends session information which has uniqueness in the data circulation system when the user apparatus sends the originality information;

the user apparatus which sends the originality information stores the originality information and the session information;

another user apparatus which receives the session information sends the session information to the user apparatus of the sending side when the another user apparatus receives the originality information; and

the user apparatus of the sending side deletes the originality information and the session information.

109. (New) A computer readable medium storing program code for causing a computer in an original data circulation system to store or circulate original data which is digital information, the computer being used as an issuer apparatus, the computer readable medium comprising:

originality information generation program code means for generating originality information which includes a fingerprint corresponding to the issues apparatus and second information corresponding to the original data; and

originality information sending program code means, for sending the originality information.

110. (New) The computer readable medium as claimed in claim 109, further comprising:

program code means for concealing a private key; and

program code means for generating a hash value of a public key corresponding to the private key as the fingerprint.

111. (New) The computer readable medium as claimed in claim 109, further comprising program code means for generating the second information by applying an unidirectional function to the original data.

112. (New) The computer readable medium as claimed in claim 111, wherein the second information is an identifier which identifies contents in a network.

113. (New) A computer readable medium storing program code for causing a computer in an original data circulation system to store or circulate original data which is digital information, the computer being used as a user apparatus, the computer readable medium comprising:

originality information sending program code means for sending originality information which includes a fingerprint corresponding to a source apparatus of the original data and second information corresponding to the original data;

identifying program code means for identifying the source apparatus of the originality information;

authentication program code means for determining that the originality information is valid if the source apparatus is authenticated and an apparatus corresponding to the fingerprint and the source apparatus are the same; and

storing program code means for storing the originality information if the authentication program code means determines that the originality information is valid.

114. (New) The computer readable medium as claimed in claim 113, further comprising program code means for deleting the originality information if the user apparatus sends the originality information to another apparatus.

115. (New) A computer readable medium storing program code for causing a computer in an original data circulation system to store or circulate original data which is digital information, the computer being used as a collector apparatus, the computer-readable medium comprising:

identifying program code means for identifying a source apparatus of originality information;

authentication program code means for authenticating the source apparatus; and

data processing program code means for performing a process corresponding to the original data if the authentication program code means determines that the originality information which is sent to the collector apparatus is valid.

116. (New) The computer readable medium as claimed in claim 115, further comprising:

program code means for storing or obtaining issuer information;

wherein the data processing program code means includes program code means for performing a process corresponding to the original data if the authentication program code means determines that the originality information which is sent to the collector apparatus is valid and if a fingerprint included in the originality information is included in the issuer information.